(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109716725 B
(45)授权公告日 2021.07.09

(21)申请号 201780056893.3
(22)申请日 2017.09.15
(65)同一申请的已公布的文献号
申请公布号 CN 109716725 A
(43)申请公布日 2019.05.03
(30)优先权数据
1615738.0 2016.09.15 GB
(85)PCT国际申请进入国家阶段日
2019.03.15
(86)PCT国际申请的申请数据
PCT/EP2017/025257 2017.09.15
(87)PCT国际申请的公布数据
WO2018/050293 EN 2018.03.22
(73)专利权人 古鲁洛吉克微系统公司
地址 芬兰图尔库
(72)发明人 托马斯·卡开宁 奥西·卡雷沃
(74)专利代理机构 北京英赛嘉华知识产权代理有限责任公司 11204
代理人 王达佐 王艳春
(51)Int.Cl.
*H04L 29/06*(2006.01)
*H04L 9/32*(2006.01)
(56)对比文件
CN 101931623 A,2010.12.29
US 2013152179 A1,2013.06.13
CN 101461209 A,2009.06.17
US 5771291 A,1998.06.23
审查员 李倩

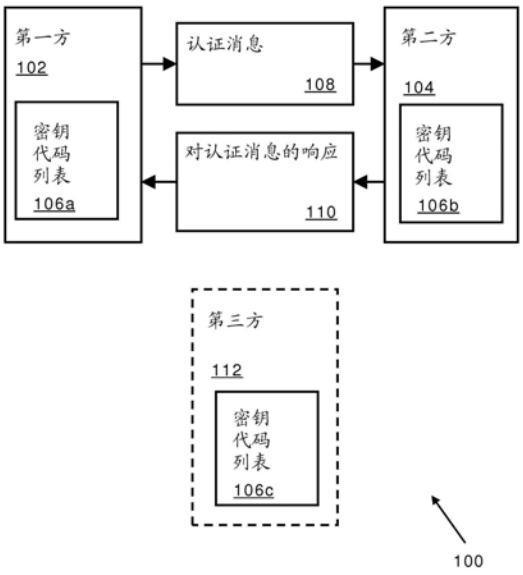
权利要求书2页 说明书18页 附图4页

(54)发明名称

数据安全系统及其操作方法和计算机可读存储介质

(57)摘要

提供了一种数据安全系统。数据安全系统至少包括经由数据通信设置相互联接的第一方和第二方,其中数据通信设置可操作为提供用户认证和/或用户登录。第一方和第二方被提供数字密钥代码列表的相同或相互兼容的副本,数字密钥代码列表包括密钥和引用密钥的索引。第一方可操作为向第二方传递认证消息,认证消息包括要导出的密钥的索引、导出密钥的数字密钥代码列表的唯一标识符(ID)、以及指示下列中至少一个的附加信息:与第一方相关联的唯一用户ID、先前从第二方接收的会话令牌、尝试用户认证和/或用户登录的日期和时间。附加信息以加密形式提供。第一方和第二方可操作为使得:当在二者间执行数据通信以提供用户认证和/或用户登录时使用密钥,密钥是基于包括在认证消息中的索引从数字密钥代码列表导出的;以及在使用后处置密钥,其中密钥设置为在第一方和第二方之间仅能够使用一次。




CN 109716725 B

1.一种数据安全系统,至少包括第一方和第二方,所述第一方和所述第二方经由数据通信设置相互联接,其中所述数据通信设置操作为提供用户认证和/或用户登录,其中:

(i)所述第一方和所述第二方提供有至少一个数字密钥代码列表的相同或相互兼容的副本,所述至少一个数字密钥代码列表被对应的唯一列表标识符ID标识并且包括密钥和引用所述密钥的索引,所述至少一个数字密钥代码列表由所述第一方或所述第二方或可信第三方提供;

(ii)所述第一方操作为向所述第二方传递认证消息,所述认证消息包括密钥的索引、要导出所述密钥的数字密钥代码列表的唯一列表ID、以及附加信息,而不是包括所述密钥,所述附加信息指示下列中至少一个:与所述第一方相关联的唯一用户ID、先前从所述第二方接收的会话令牌、尝试用户认证和/或用户登录的日期和时间,其中所述附加信息以加密形式提供,其中所述认证消息中包括的唯一列表ID唯一地标识将要使用多个所述数字密钥代码列表中的哪个来导出待用于解密的所述密钥;以及

(iii)所述第二方操作为:验证所接收的唯一列表ID是否与所述第二方所具有的一个数字密钥代码列表的唯一列表ID相同,并验证所接收的索引是否与所述第二方的具有与所接收的唯一列表ID相同的唯一列表ID的数字密钥代码列表中所包括的索引之一相同;

所述第一方和所述第二方操作为:当在二者间执行数据通信以提供用户认证和/或用户登录时,使用基于包括在所述认证消息中的唯一列表ID和索引而从具有与包括在所述认证消息中的唯一列表ID相同的唯一列表ID的数字密钥代码列表导出的与包括在所述认证消息中的索引对应的密钥;以及在使用后处置所述密钥,其中所述密钥设置为在所述第一方和所述第二方之间仅能够使用一次。

2.根据权利要求1所述的数据安全系统,其中,所述密钥被选择为供以下任何一方使用:所述第一方、所述第二方或可信第三方。

3.根据权利要求1或2所述的数据安全系统,其中,所述第一方和所述第二方是相互授权和认证的。

4.根据权利要求1所述的数据安全系统,其中,当所述数字密钥代码列表由所述可信第三方提供时,所述第一方操作为匿名地执行所述数据通信。

5.根据权利要求1所述的数据安全系统,其中,所述数据安全系统操作为:允许基于与所述第一方和所述第二方相关联的用户的生物识别来访问所述数字密钥代码列表。

6.根据权利要求1所述的数据安全系统,其中,所述数据安全系统操作为:在发现安全性已受到变得可供未授权第三方使用的给定数字密钥代码列表有关的信息的危害时,停用所述给定数字密钥代码列表。

7.根据权利要求1所述的数据安全系统,其中,所述数据安全系统操作为:将到期时间与给定数字密钥代码列表相关联,并且在到达所述到期时间时停用所述给定数字密钥代码列表。

8.一种操作数据安全系统的方法,所述数据安全系统至少包括经由数据通信设置相互联接的第一方和第二方,其中所述数据通信设置操作为提供用户认证和/或用户登录,所述方法包括:

(a)为所述第一方和所述第二方提供被唯一列表标识符ID标识的至少一个数字密钥代码列表的相同或相互兼容的副本,所述数字密钥代码列表包括密钥和引用所述密钥的索

引,所述至少一个数字密钥代码列表由所述第一方、所述第二方或可信第三方提供;

(b)设置所述第一方使其操作为向所述第二方传递认证消息,所述认证消息包括密钥的索引、要导出所述密钥的数字密钥代码列表的唯一列表ID、以及附加信息,而不包括所述密钥,所述附加信息指示下列中至少一个:与所述第一方相关联的唯一用户ID、先前从所述第二方接收的会话令牌、尝试用户认证和/或用户登录的日期和时间,其中所述附加信息以加密形式提供,其中所述认证消息中的唯一列表ID唯一地标识将要使用多个所述数字密钥代码列表中的哪个来导出待用于解密的所述密钥;以及

(c)设置所述第二方使得所述第二方操作为:验证所接收的唯一列表ID是否与所述第二方所具有的一个数字密钥代码列表的唯一列表ID相同,并验证所接收的索引是否与所述第二方的具有与所接收的唯一列表ID相同的唯一列表ID的数字密钥代码列表中所包括的索引之一相同;

设置所述第一方和所述第二方使得操作为:当在二者间执行数据通信以提供用户认证和/或用户登录时,使用基于包括在所述认证消息中的唯一列表ID和索引而从具有与包括在所述认证消息中的唯一列表ID相同的唯一列表ID的数字密钥代码列表导出的与包括在所述认证消息中的索引对应的密钥;以及在使用后处置所述密钥,其中所述密钥设置为在所述第一方和所述第二方之间仅能够使用一次。

9.根据权利要求8所述的方法,其中,所述方法包括设置所述密钥被选择为供以下任何一方使用:所述第一方、所述第二方或可信第三方。

10.根据权利要求8所述的方法,其中,所述方法包括使所述第一方和所述第二方相互授权和认证。

11.根据权利要求8所述的方法,其中,所述方法包括当所述数字密钥代码列表由所述可信第三方提供时,设置所述第一方操作为匿名地执行所述数据通信。

12.根据权利要求8所述的方法,其中,所述方法包括设置所述数据安全系统操作为:允许基于与所述第一方和所述第二方相关联的用户的生物识别来访问所述数字密钥代码列表。

13.根据权利要求8所述的方法,其中,所述方法包括设置所述数据安全系统操作为:在发现安全性已受到变得可供未授权第三方使用的给定数字密钥代码列表有关的信息的危害时,停用所述给定数字密钥代码列表。

14.根据权利要求8所述的方法,其中,所述方法包括设置所述数据安全系统操作为:将到期时间与给定数字密钥代码列表相关联,并且在到达所述到期时间时,停用所述给定数字密钥代码列表。

15.一种非暂时性计算机可读存储介质,其上存储有计算机可读指令,其特征在于,所述计算机可读指令在被处理器执行时实现如权利要求8至14中任一项所述的方法的步骤。

# 数据安全系统及其操作方法和计算机可读存储介质

## 技术领域

[0001] 本公开涉及数据安全系统。此外，本公开还涉及操作前述数据安全系统的方法。此外，本公开还涉及计算机程序产品，该计算机程序产品包括其上存储有计算机可读指令的非暂时性计算机可读存储介质，计算机可读指令可由计算机化设备执行，计算机化设备包括用于执行前述方法的处理硬件。

## 背景技术

[0002] 在数字计算机和信息系统被发明之前几个世纪之久，密码已经被用来增强安全性。例如，在罗马时代信使之间使用预先商定的密码用于身份验证；在战场上口令被用以验证接近岗哨的人是友军而非敌人。当代信息社会严重依赖于密码的使用，例如用于登录(即，验证)计算机、登录智能电话、启动电视、访问支付终端、将数据输入自助服务自动售货机等等。此外，密码同时也在许多不同的社会服务和社交媒体服务、在线银行、操作系统、电子邮件服务器中被用于验证用户的真实性。

[0003] 为了提高当代数字信息系统的安全性，传统的做法是采用多种不同的安全方法，例如：

[0004] (i)基本访问认证(Basic Auth，参见参考文献[1])；

[0005] (ii)摘要访问认证(参见参考文献[2])；

[0006] (iii)Kerberos协议(参见参考文献[3])；

[0007] (iv)NT局域网管理器(参见参考文献[4])；

[0008] (v)开放授权(参见参考文献[5])；

[0009] (vi)开放ID(参见参考文献[6])；

[0010] (vii)简单和受保护的GSSAPI协商机制(SPNEGO，参见参考文献[7])；

[0011] (viii)安全远程密码协议(SRP，参见参考文献[8])；

[0012] (ix)传输层安全(TLS)客户端认证握手(参见参考文献[9])，

[0013] 等等。上述(i)至(ix)项中包括商标。

[0014] 当前几乎所有基于密码的保护方法都存在已知的技术缺陷。然而，由于各种信息的泄露、针对大型数据服务供应商的数据的安全漏洞和披露，信息安全技术近年来取得了相当大的进展。在实践中，这些漏洞、泄漏和披露已迫使信息安全专家设计新型的安全方法。

[0015] 众所周知，使用密码是必要的，但是这在依赖于信息系统的现代社会中会引起各种问题。无论采用何种类型的信息系统或何种类型的数据安全配置，这些信息系统的用户最终都会因为他们的不了解或不重视而造成在数据安全和信息安全上的漏洞。几乎每天都会有关于用户账户受损、密码泄露、各类以返回从受损的用户账户中窃取的个人私人信息来敲诈金钱的恶意软件等等新闻发布。

[0016] 目前已知的用户认证技术是基于使用加密数据通信连接将用户标识和/或密码传送到服务供应商的服务器或终端设备，其中安全性主要基于可信方提供的证书。当下众所

周知的是,加密连接无法保证用户至关重要的登录(即,验证)信息在未加密状态下不被恶意未授权方获取;只要传送链中的一个薄弱环节就可能足以将重要登录信息泄露给恶意未授权方。

[0017] 尽管采取了保护数据的措施,但众所周知互联网®(依据互联网协议 (IP)例如传输控制协议(TCP)和用户数据报协议(UDP)操作,但不限于此)作为全球信息网络不仅可以供超级大国,也可以供许多跨国公司窥探人们并追踪他们的活动,这是由于每次使用当代信息系统时都会留下数字元痕迹。这些数字元痕迹或被动数字足迹总是有很大可能被追踪并与可能是例如法人的个人独立用户相连接。在给予足够计算资源的情况下,追踪甚至可以被追溯执行。

[0018] 同样众所周知的是,目前的国家立法不能确实地影响跨国的软件设置,这些设置将其相关联的认证,即其相关联的登录(即,验证)进程集中到生产者的服务器上,而这些服务器通常驻留在外国领土内,其法规可能因此与实际使用该服务的国家的立法相冲突。因此,互联网已经变为一种新型战争的战场,在这一战场上一些国家试图通过新的法律来保护其公民,这些法律将阻止其公民使用由外国控制的基础设施(即,网络节点和服务器)提供的服务,表面上出于国家安全的原因。换言之,涉及国际协议的国家法律的变化可能会产生安全不确定性,例如,在给定数据服务器集中于一个国家,而与给定数据服务器交互的其他国家中没有统一规则的情况下。

[0019] 此外,当前的问题是个人账户被破解或个人敏感信息被盗。然而,当前往往没有简单而切实的办法解决这些问题。此外,对于许多用户来说,无论是抽象意义上的还是就技术程序而言,通常几乎不可能适应使用复杂的工具和程序,例如使用良好隐私(PGP®)模型或类似类型的加密来加密电子邮件。因此在实践中,最好不应把保护他或她的信息免受恶意软件和未授权方获取的主要责任交给给定用户,因为当代用户的范围覆盖幼儿到老年人;而这些人在满足他们的各种在线需求,例如社交媒体互动和在线购物活动时,很少关注安全问题。

[0020] 在已公布的美国专利文献US 2013/152179 A1(LEE等人;“使用一次性识别的用户认证系统和方法”)中,描述了一种使用一次性识别 (OTID)进行用户认证的系统,包括客户端终端,配置为生成在用户认证中使用的多个OTID,并且在每个认证会话中顺序地选择所生成的 OTID中的一个以使用所选择的OTID作为用户标识。此外,该系统包括:认证服务器,配置为从客户端终端接收并存储所生成的OTID;当接收到所选择的OTID和机密密钥时,在数据库中查询OTID,并确定与所查询 OTID相关联并存储在数据库中的机密密钥是否与所接收的机密密钥匹配,以执行用户认证。

[0021] 在已公布的WO专利文献WO 2007/117131 A1(信托综合服务公司;“用于安全数据传输的设置和方法”)中,描述了一种用于客户端和第三方计算机设置之间的安全数据传输的方法和系统。方法包括:a)通过安全性服务器经由传送会话认证客户端的用户;b)由安全性服务器提供密钥对,密钥对包括公钥和私钥;c)在使用密钥对的同时,在客户端和第三方计算机设置之间执行安全数据传输。密钥对具有由以下定义的有限寿命:预定的持续时间、或预定数量的传送会话、或预定数量的动作。

[0022] 在已公布的美国专利文献US 2008/034216 A1(Eric Chun Wah Law (US);“在使

用连续的一次性密码的双方之间的相互认证和安全信道建立”)中,描述了一种配置用于双方之间的相互认证和安全信道建立的传送系统和方法。第一方生成第一个一次性密码并将其发送给第二方。第二方通过使用相同的算法、机密和参数生成一次性密码来认证第一方,并将其与接收的第一个一次性密码匹配。如果接收到的第一个一次性密码与生成的密码匹配,则第二方生成连续的一次性密码,并使用连续的一次性密码建立到第一方的安全信道。第一方通过使用安全信道与第二方成功传送来生成连续的一次性密码并认证第二方。

[0023] 在已公布的EP专利文献EP2911365(A1)(Dejamobile(FR);“用于保护由用户的移动设备和接受点之间的多个服务提供的交易的方法和系统”)中,描述了一种用于在用户的移动设备和接受点之间保护服务的交易的方法。方法包括在安全性服务器上为给定服务和用户服务创建至少一个令牌,每个令牌具有值,其中每个令牌被加密。方法还包括由安全性服务器将加密的令牌传送到移动设备,以及在移动设备和接受点之间的交易期间将加密的令牌存储在移动设备上。方法还包括将先前存储的加密的令牌从移动设备传送到接受点。方法还包括在接受点处解密加密的令牌,以及验证解密的令牌对于交易是有效的。

## 发明内容

[0024] 本公开旨在提供一种改进的数据安全系统。

[0025] 此外,本公开旨在提供一种改进的操作数据安全系统的方法。

[0026] 如上所述,本公开的另一目的在于至少部分地克服现有技术的至少一些问题。

[0027] 第一方面,本公开的实施例提供了一种数据安全系统,其至少包括第一方和第二方,所述第一方和第二方经由数据通信设置相互联接,其中可操作所述数据通信设置以提供用户认证和/或用户登录,其中:

[0028] (i)所述第一方和第二方提供有至少一个数字密钥代码列表的相同或相互兼容的副本,所述数字密钥代码列表包括密钥和引用密钥的索引;

[0029] (ii)所述第一方可操作为向所述第二方传递认证消息,所述认证消息包括密钥的索引、要导出所述密钥的数字密钥代码列表的唯一标识符(ID)、以及附加信息,而不包括所述密钥,所述附加信息指示下列中至少一个:与所述第一方相关联的唯一用户ID、先前从所述第二方接收的会话令牌、尝试用户认证和/或用户登录的日期和时间,其中所述附加信息以加密形式提供;以及

[0030] (iii)可操作第一方和第二方使得:当在二者间执行数据通信以提供用户认证和/或用户登录时使用密钥,所述密钥是基于包括所述认证消息中的索引从所述数字密钥代码列表导出的;以及在使用后处置所述密钥,其中所述密钥设置为在所述第一方和第二方之间仅能够使用一次。

[0031] 本公开的优点在于,可操作第一方和第二方使得在它们之间执行数据通信,而不需要加密或保护正在使用的密钥或其索引,因为密钥是一次性的并且仅能够使用一次。

[0032] 根据本公开的实施例,用户认证和/或用户登录是自动执行的,无需任何用户动作,因为不需要传递密码。

[0033] 第二方面,本公开的实施例提供了一种操作数据安全系统的方法,所述数据安全系统至少包括经由数据通信设置相互联接的第一方和第二方,其中可操作所述数据通信设置以提供用户认证和/或用户登录,所述方法包括:

[0034] (a)向所述第一方和第二方提供至少一个数字密钥代码列表的相同或相互兼容的副本,所述数字密钥代码列表包括密钥和引用密钥的索引;

[0035] (b)设置所述第一方可操作为向所述第二方传递认证消息,所述认证消息包括密钥的索引、要导出所述密钥的数字密钥代码列表的唯一标识符(ID)、以及附加信息,而不包括所述密钥,所述附加信息指示下列中至少一个:与所述第一方相关联的唯一用户ID、先前从所述第二方接收的会话令牌、尝试用户认证和/或用户登录的日期和时间,其中所述附加信息以加密形式提供;以及

[0036] (c)设置所述第一方和第二方可操作为:当在二者间执行数据通信以提供用户认证和/或用户登录时使用密钥,所述密钥是基于包括在所述认证消息中的索引从所述数字密钥代码列表导出的,以及在使用后处置所述密钥,其中所述密钥设置为在所述第一方和第二方之间仅能够使用一次。

[0037] 第三方面,本公开的实施例提供了一种计算机程序产品,该计算机程序产品包括其上存储有计算机可读指令的非暂时性计算机可读存储介质,所述计算机可读指令可由计算机化设备执行,所述计算机化设备包括用于执行根据前述第二方面的方法的处理硬件。

[0038] 根据结合所附权利要求解释的说明性实施例的附图和详细描述,本公开的其他方面、优点、特征和目的将变得显而易见。

[0039] 应当理解,在不脱离由所附权利要求限定的本公开的范围的情况下,本公开的特征易于以各种组合进行组合。

## 附图说明

[0040] 当结合附图阅读时,可以更好地理解以上发明内容以及说明性实施例的以下详细描述。出于说明本公开的目的,在附图中示出了本公开的示例性构造。然而,本公开不限于本文公开的具体方法和装置。此外,本领域技术人员将理解附图不是按比例绘制的。在可能的情况下,类似的元素均由相同的数字表示。

[0041] 现在将参考以下附图仅通过示例的方式描述本公开的实施例,其中:

[0042] 图1是根据本公开实施例的数据安全系统的示意图;

[0043] 图2A是根据本公开实施例的,描述了操作图1的数据安全系统的方法的各步骤的流程图的示意图;

[0044] 图2B是根据本公开实施例的,描述认证过程的步骤的流程图的示意图;以及

[0045] 图3是根据本公开实施例的示例性认证消息的内容的图示。

[0046] 在附图中,下划线数字用于表示下划线数字所在的项或与下划线数字相邻的项。当数字没有下划线并伴有相关箭头时,未加下划线的数字用于标识箭头指向的一般项。

## 具体实施方式

[0047] 以下详细描述示出了本公开的实施例以及可以实现它们的方式。尽管已经公开了执行本公开的一些模式,但是本领域技术人员将认识到其他实施例也可以用于执行或实践本公开。

[0048] 在下文中,提供了本公开的示例性实施例的描述,其中在描述中使用了如下缩略词和定义:

[0049] Basic Auth(基本认证):在给定示例性HTTP(超文本传输协议)交易中,基本访问认证用于HTTP用户代理以在发出请求时提供用户名和密码。

[0050] Digest Auth(摘要认证):摘要访问认证是多个商定的方法中的一个,网络服务器可以使用该方法来协商与用户的网络浏览器相关的凭据,诸如用户名或密码。

[0051] Kerberos:一种基于“票证”工作的计算机网络认证协议。

[0052] NFC:近场通信,通常是近场无线通信,例如BlueTooth®。当前的近场通信通常使用mW量级的无线传输功率提供高达100米的无线通信范围。

[0053] NTLM:一套为用户提供认证、完整性和机密性的Microsoft安全协议。

[0054] OAuth:开放标准和分散式认证协议。

[0055] OpenID:允许用户通过合作站点使用第三方服务进行认证。

[0056] PGP:良好隐私,即当前加密和解密软件产品。

[0057] GPG:GNU隐私防护是PGP的免费软件替代品。

[0058] PKI:公钥基础设施。

[0059] SPNEGO:简单且受保护的GSSAPI协商机制;客户端-服务器软件设置使用GSSAPI“伪机制”来协商安全技术的选择。

[0060] SRP:安全远程密码协议(SRP)是一种增强的密码认证密钥协商 (PAKE)协议。

[0061] TLS:传输层安全客户端,即经过认证的TLS握手设置。

[0062] 上述缩略词可能包括商标。

[0063] 第一方面,本公开的实施例提供了一种数据安全系统,其至少包括第一方和第二方,第一方和第二方经由数据通信设置相互联接,其中可操作数据通信设置以提供用户认证和/或用户登录,其中:

[0064] (i)第一方和第二方提供有至少一个数字密钥代码列表的相同或相互兼容的副本,数字密钥代码列表包括密钥和引用密钥的索引;

[0065] (ii)第一方可操作为向第二方传递认证消息,认证消息包括要导出的密钥的索引、要导出密钥的数字密钥代码列表的唯一标识符(ID)、以及附加信息,附加信息指示下列中至少一个:与第一方相关联的唯一用户ID、先前从第二方接收的会话令牌、尝试用户认证和/或用户登录的日期和时间,其中附加信息以加密形式提供;以及

[0066] (iii)第一方和第二方可操作为:当在二者间执行数据通信以提供用户认证和/或用户登录时使用密钥,密钥是基于包括在认证消息中的索引从数字密钥代码列表导出的;以及在使用后处置密钥,其中密钥设置为在第一方和第二方之间仅能够使用一次。

[0067] 在整个本公开中,术语“第一方”或术语“第二方”用于指代由所识别的用户所有和使用的企业、个人或软件组件。在本公开的示例性实施例中,第一方和第二方中的至少一方是服务,例如数据传递服务、内容传递服务、银行服务、财务交易服务等。此外,软件组件可以是例如软件应用程序、软件应用程序的一部分、为其他软件应用程序提供操作环境的软件层(例如,通信协议栈中的支持层)。

[0068] 应当理解,本文中的术语“第一”、“第二”和类似术语不表示任何特定的功能或顺序或重要性,而是用于区分一方与另一方。换而言之,第一方和第二方可以在给定的时间点分别充当发送方和接收方,并且可以在另一时间点分别充当接收方和发送方。

[0069] 根据本公开的实施例,用户认证和/或用户登录是自动执行的,无需任何用户动

作,因为在这种操作模式下不需要传递密码。相反,第一方可操作为向第二方传递密钥索引(即,一次性密钥的索引)以及认证消息中的前述附加信息。

[0070] 可选地,数字密钥代码列表的唯一ID是分配给数字密钥代码列表的序列号。

[0071] 可选地,使用其索引在认证期间传递的精确加密密钥来加密附加信息。或者,可选地,使用一些其他加密密钥来加密附加信息,例如密钥代码列表中的下一个密钥,在这种情况下,第二方已经知道使用下一个密钥这一事实。再者,可选地,附加信息使用其索引被单独传递的另一加密密钥加密。

[0072] 如前所述,附加信息指示下列至少一个:与第一方相关联的唯一用户ID、先前从第二方接收的会话令牌、尝试用户认证和/或用户登录的日期和时间。应当理解,如果数字密钥代码列表已经引用唯一用户ID,则唯一用户ID是可选的(即,无需传递)。换而言之,如果数字密钥代码列表是唯一密钥代码列表并且被识别为与唯一用户ID相关联,则无需传递唯一用户ID。可选地,就此而言,在向第一方和第二方提供数字密钥代码列表的相同或相互兼容的副本时,数字密钥代码列表与唯一用户ID 相关联。

[0073] 在认证中发送指示会话令牌或日期和时间的附加信息是有利的,从而可以验证密钥已被正确使用并且认证消息未过时。

[0074] 在本公开全文中,术语“会话令牌”指的是由第二方生成并发送到第一方以识别第一方和第二方之间的当前交互会话的唯一会话标识符。可选地,第二方可操作为在交互会话开始时生成会话令牌并将其发送至第一方,其中会话令牌以加密形式发送。可选地,就此而言,第二方可操作为使用来自数字密钥代码列表的加密密钥来加密会话令牌,并将加密密钥的索引发送至第一方。可选地,第一方和第二方可操作为基于索引使用加密密钥,并且在使用之后处置加密密钥,其中加密密钥设置为在第一方和第二方之间仅能够使用一次。

[0075] 这种会话令牌在希望当前登录会话在预定时间段内或直到满足预定目标为止保持开放(即,活跃)的情况下特别有利。例如,给定的登录会话可以在预设的不活跃时间之后到期,预设的不活跃时间可以是几分钟到几小时。又例如,给定的登录会话可以在客户于在线商店上下订单之后到期。

[0076] 可选地,当在相同交互会话期间执行后续数据通信通信时,第一方可操作为发送后续数据以及指示会话令牌的附加信息。可选地,在这种情况下,至少附加信息以加密形式提供。可选地,后续数据和附加信息都以加密形式提供。

[0077] 应当理解,例如,当第一方是客户端而第二方是服务器时,通常使用会话令牌。可选地,在这种情况下,第一方(例如,客户端)仅需要存储和处理会话令牌,而与当前交互会话相关的所有会话数据均链接到会话令牌,并存储在第二方(例如,在与服务器关联的数据库中)。通常,客户端不会直接访问存储在服务器上的会话数据。此外,可选地,第二方可操作为以压缩形式存储会话数据,以便提高效率并允许存储更多会话数据。在这种情况下,第二方可操作为在从第一方接收到指示会话令牌的信息时稍后解压缩会话数据。

[0078] 此外,可选地,数字密钥代码列表通过密钥容器或密钥生成器实现,密钥容器或密钥生成器能够基于其索引存储和/或生成一次性密钥。

[0079] 应当理解,在本公开中被称为“密钥代码列表”的概念的各种不同实现仅是这样的密钥代码列表(也称为“密钥容器”或“密钥生成器”) 可以被实现的几个示例;许多其他方式也是可能的。用于本公开中使用的密钥的列表的术语是“密钥代码列表”,但是应当理解,

它可以指代多种类型的实现。其中一个实现可以是包含索引和索引所引用的密钥的列表。另一种实现可以是一个密钥生成器，该密钥生成器被发送密钥索引的信号，然后，密钥生成器可重复和可再现地返回与索引匹配的密钥，即，密钥生成器总是生成具有相同索引的相同密钥。

[0080] 可选地，就此而言，数字密钥代码列表通过数字加密密钥钱包实现，例如专利文献PCT/EP2016/025042(申请人-古鲁洛奇微系统公司 (Gurulogic Microsystems Oy))中描述的加密密钥钱包，其中详细描述了一种设置如何直接地或通过可信第三方生成可在两个或多个通信方之间安全使用的加密密钥钱包。这种密钥钱包可选地是动态密钥代码列表。

[0081] 可选地，静态地提供数字密钥代码列表。

[0082] 应当理解，本公开的实施例涉及例如，在一个或多个登录进程，例如在多个登录进程中使用的认证。在操作中，数据以加密形式安全地传递，其中通常从一个给定用户到另一个给定用户或服务实现与数据相关联的认证。然而，可选地，根据本公开的实施例，为了使用软件组件或模块，对设备进行认证，或者对软件组件或模块(例如应用程序、服务或子例程)进行认证。

[0083] 此外，可选地，使用在一个或多个部分中选择性地插入到认证消息中的一个或多个字符或数字来传递给定密钥的索引。应当理解，通常，与发送密钥本身相比，只需要较少的比特来发送引用密钥的索引。而且，应当理解，即使密钥是加密的，发送密钥索引而不是密钥本身也更为安全。

[0084] 根据本公开的实施例，密钥被选择供以下任何一个使用：第一方、第二方或可信第三方。在一些实现中，第一方(即，发送方)选择要使用的密钥。在其他实现中，可信第三方选择要使用的密钥，并且向第一方和第二方传送引用所选密钥的密钥索引。

[0085] 在其他实现中，第二方(即，接收方)选择要使用的密钥，并且向第一方传送引用所选密钥的密钥索引。应当理解，所选密钥从不被传递；相比之下，密钥的传递是已知类型的数据安全系统的操作特性。

[0086] 可选地，在已知第一方和第二方具有同一数字密钥代码列表的相同的或兼容的副本的情况下，第一方(即，发送方)可操作为独立于第二方(即，接收方)而选择要使用的密钥；例如，“兼容”是指密钥代码列表彼此不同，但是能够协同使用以实现本公开的实施例。或者，可选地，如果不知道第一方和第二方是否被提供相同的数字密钥代码列表的相同副本，或者如果数据通信中所使用的方法需要，则在第一方和第二方之间进行协商以确认将使用哪个密钥。

[0087] 根据本公开的实施例，第一方可操作为使用尚未提供给第二方的密钥。在这种情况下，密钥是从数字密钥代码列表的生产者实时地或几乎实时地(例如，在几秒钟内(例如，小于60秒))获取的。这种操作方式允许第一方和第二方登录各种信息系统和服务，例如由可信第三方授权的信息系统和服务。可选地，通过利用常规登录方法，一方可操作为向另一方传递数字密钥代码列表，数字密钥代码列表用于稍后在第一方和第二方之间执行的登录过程。

[0088] 此外，如果第二方(即，接收方)知晓(即，具有使接收方能够确定的信息)要使用的密钥或其索引，则无论密钥是由第二方还是由可信第三方选择，第一方(即，发送方)甚至不需要将密钥索引与要传送的数据(例如登录(即，验证)信息)一起发送，或者在被传送给第

二方 (即,接收方)的认证消息中发送。然而,即使在第二方(即,接收方) 知晓(即,具有使接收方能够确定的信息)密钥索引的情况下,发送密钥索引通常也是有利的,以避免几次登录(即,验证)尝试或在短时间内发出或接收的若干消息之间的混淆。

[0089] 根据本公开的实施例,第一方和第二方可操作为在无需加密或保护密钥索引的情况下在二者间执行数据通信,。应当理解,当传统方法涉及在各方之间传递密钥时,密钥需要以加密形式传送;然而,当根据本公开的实施例传送时,密钥的索引不需要以加密的形式传递。在本公开的一些实施方式中,发送方在发起与接收方的交互时不一定需要发送任何信息,而仅需要进行第一次接触;在这种情况下,当双方之间的交互已经发起时,双方以根据本公开实施例的方式进行通信,即发送消息。

[0090] 在传统的已知系统的示例性场景中,相比之下,在恶意第三方设法劫持认证消息的情况下,恶意第三方能够在登录信息(包括用户密码) 和用于加密登录信息的密钥在消息中传递且密钥未加密的情况下,使用该消息登录。

[0091] 相比之下,根据本公开的实施例,避免了用户标识和密码的传输和传递。应当理解,除了密钥索引和数字密钥代码列表的唯一标识之外,发送上述附加信息是有利的,从而使得认证更加安全。如前所述,可以使用密钥索引引用的密钥、密钥代码列表中的下一个密钥或其索引单独被传递的另一个加密密钥来加密这样的附加信息。

[0092] 应当理解,根据本公开的实施例,由于没有获得可用于识别第一方和第二方的关于第一方和第二方的此类信息,可以使用公开不受保护的网络连接来执行整个登录(即,验证)进程。此外,由于密钥是一次性的并且仅能够使用一次,因此恶意方甚至不能追溯地跟踪和记录授权第一方和第二方之间的登录进程。然而,应当理解,在本公开的实施例中,期望的是,不能从早期的密钥轻易地预期到之后的密钥;换而言之,后续的密钥最好不是来自早期密钥的简单数学累进,使得恶意第三方可以识别密钥在时间演变中的趋势。可选地,所采用的密钥的序列在取值上随机地(即,任意地或伪任意地)变化。

[0093] 这里应理解的是,第一方和第二方使用的密钥可以追溯地被破坏。但是,密钥在将来登录时既不可用,也不能用于破解过去的登录,因为登录期间使用的密钥是一次性的,且仅能够使用一次,即只能使用一次。因此,在本公开的实施例中,即使可能被恶意第三方攻击,消息中也不包含可以如此重复使用的任何这样的信息(例如,诸如用户ID以及密码)。下一次,消息在任何情况下都需要使用不同的密钥加密。因此,信息实现为使得其之后不能用于登录到相应的系统或任何其他系统。

[0094] 此外,可选地,第一方和第二方可操作为使用相同的密钥来加密在登录过程之后传送的附加信息和后续数据。或者,可选地,选择不同的密钥用于认证和后续数据通信。可选地,就此而言,后续数据通信使用密钥代码列表中的下一个密钥,在这种情况下,接收方已经知晓使用下一个密钥这一事实。或者,可选地,后续数据通信使用另一加密密钥,其索引是单独传递的。可选地,针对所传送的每个消息更改密钥。因此,它们的索引也针对所传送的每个消息而改变。索引要么被传递,要么被接收方含蓄地知晓,即密钥以特定的顺序使用。在这种情况下,第一方和第二方在登录(即,验证)过程和随后数据通信期间采用相同的加密算法。这使得能够直接使用数字密钥代码列表,并且可能确保简单且整齐的功能以及登录过程和后续数据通信的完全整合。这也使得可以在第一方和第二方之间实现更为安全和不复杂的通信设置。与用于提供数据安全性的传统已知的方法相比,这种操作是非常有

利的，其中传统已知的方法在操作中采用由几个不同供应商设计和/或制造的表面上安全的若干组件，但是由于这些部件缺乏技术实现和各种接口之间的整合，其整体保护性降低了。

[0095] 根据本公开的实施例的数据安全系统不仅保护登录过程，还保护用户认证。在登录过程中，当然地会进行对于给定用户的用户识别。但是，同时也检测给定用户的用户权限。

[0096] 数据安全系统可操作为相互验证软件组件，这创建了用于保护数据和用于认证用户的、与独立于设备且与独立于平台的系统。

[0097] 应当理解，旨在独立于平台的数据安全系统的实际实现被有利地设计为全面安全解决方案，其包含硬件和相关的周围的“生态系统”之间的各种接口。这种全面安全解决方案不允许使用不够安全的组件，即在数据安全性方面是薄弱环节的组件。为此，本公开的实施例的一个实现单独或组合地使用设备制造商打算使用的一个或多个安全措施，例如，使用指纹读取器、语音识别、虹膜识别、基因组数据和类似识别方式的对于用户的生物识别。可以理解，用户不需要输入任何主密码；相反，数据安全系统是基于可以使用设备制造商提供的接口读取的唯一个人信息。采用生物识别使得用户设备可以验证在生态系统中操作的软件设置，并允许该软件设置访问包括密钥及其相应索引的数字密钥代码列表。这种用户设备的示例包括但不限于移动电话、智能电话、个人可穿戴电子数字设备(例如，智能手表)、移动互联网设备(MID)、平板电脑、超移动个人计算机(UMPC)、平板手机电脑、个人数字助理(PDA)、网络平板电脑、个人电脑(PC)、掌上电脑、笔记本电脑、台式电脑和诸如游戏机、电视(TV)和机顶盒(STB)等的互动娱乐设备。

[0098] 因此，根据本公开的实施例，数据安全系统可操作为允许基于与第一方和第二方相关联的用户的生物识别来访问数字密钥代码列表。作为示例，在智能电话中，用户可以使用他/她的指纹来获得提供给智能电话的数字密钥代码列表的访问权限。

[0099] 根据本公开的实施例，第一方和第二方是相互授权和认证的。

[0100] 根据本公开的另一实施例，数字密钥代码列表由第一方或第二方提供。

[0101] 根据本公开的另一实施例，数字密钥代码列表由可信第三方提供。

[0102] 此外，可选地，通过使用加密的电子邮件消息(例如，通过使用诸如GNU隐私防护之类的方法；参见参考文献[12])将数字密钥代码列表传递给第一方和/或第二方。

[0103] 可选地，当数字密钥代码列表由可信第三方提供时，第一方(即，发送方)可操作为匿名地执行数据通信。在这种情况下，即使第一方和第二方在操作中匿名地通信，第一方和第二方也被可信第三方确认为授权方。换而言之，例如关于登录(即，验证)，当希望第一方(即，发送方)对第二方(即，接收方)保持匿名，但仍然保持被信任时，向第一方和第二方提供由可信第三方生成的数字密钥代码列表，由此第一方和第二方使用从可信第三方提供的数字密钥代码列表导出的密钥。

[0104] 但是，如果第一方和第二方希望对其他第三方保持匿名，则向第一方和第二方提供由第一方和第二方之一生成的数字密钥代码列表，由此第一方和第二方使用由该数字密钥代码列表导出的密钥。在这种情况下，即使第一方和第二方彼此知晓，也没有第三方能知晓谁在与谁进行通信。特别是在给定服务供应商(即接收方)希望识别服务用户(即发送方)的情况下，使用这种方法是有利的，例如在登录过程期间，给定服务供应商和服务用户可操

作为使用由服务供应商生成和提供的数字密钥代码列表。

[0105] 可选地，由可信第三方生成的第一数字密钥代码列表与由第一方和第二方中的任何一方生成的第二密钥代码列表以混合密钥设置的形式组合使用。

[0106] 有利地，数字密钥代码列表的生产者独立地生成非常强的密钥并将这些密钥存储到数字密钥代码列表中。

[0107] 总的来说，本公开的实施例可操作为使得经由公用互联网®例如采用互联网协议(IP)执行的交易更为安全。在本公开的实施例中，与发送方相关联的用户在登录由接收方提供的服务时，不需要处理即不需要关注用户标识和/或密码。认证消息潜在地可以包括任何可想到的信息；然而，有利地，采用明智的(即，适当的)信息，使得信息不需要包括与登录服务的特定方相关联用户的用户ID和密码，但足以识别特定方，即用于用户认证。就此而言，认证消息包括正在使用的数字密钥代码列表的唯一ID、来自数字密钥代码列表的密钥索引、以及指示下列中至少一个的附加信息：与特定方相关联的唯一用户ID、从服务接收的会话令牌、尝试用户认证和/或用户登录的日期和时间，其中附加信息以加密形式提供。

[0108] 在本公开的实施例中，当向两个发送方提供多个数字密钥代码列表时，随后通常需要两个发送方在彼此间关于以安全方式例如加密和/或模糊的方式交换数据时使用多个数字密钥代码列表中的哪一个而交换信息。采用多个可能的密钥代码列表的这种方法可以用于在本公开的实施例中进一步增强安全性。此外，当在先的密钥代码列表变得穷尽时，在两个发送方之间有利地共享新的密钥代码列表。在这种情况下，要使用的密钥代码列表的ID将唯一地标识正在使用哪个密钥代码列表。

[0109] 即使没有使用密码，在本公开的实施例中，也可以根据提供给定服务的每个国家的法规来识别和认证每个用户；例如，某些国家的法规可能指示安全部门检查数据，以侦查任何恐怖主义活动。根据本公开的实施例，数据安全系统致力于集中地控制数字密钥代码列表，这意味着数据安全系统可使用户能够安全地登录并使用外国服务，同时将他/她的全部信息存储到根据当地(即，国家)立法维护的数据存储器。因此，认证消息不会对其用户或相关服务供应商或正在使用该服务的国家构成威胁。

[0110] 可以理解，在检测到密钥代码列表用于恶意目的的情况下，可以使密钥代码列表无效；换而言之，具有该特定ID的密钥代码列表可以不再用于认证或注册服务。

[0111] 可选地，就此而言，数据安全系统可操作为在发现安全性已受到变得可供未授权第三方例如黑客使用的数字密钥代码列表有关的信息的危害时，停用给定数字密钥代码列表。这种停用可选地响应于停用命令而实现，包括要停用的给定数字密钥代码列表的标识。可选地，停用命令由以下至少一个发出：第一方、第二方、负责监督发生在第一方和第二方之间的通信的安全性的第三方。

[0112] 此外，可选地，数据安全系统可操作为：将到期时间与给定数字密钥代码列表相关联，以及在到达到期时间时停用给定数字密钥代码列表。

[0113] 本公开的实施例增加了安全性，因为交易仅在授权方和认证方之间发生，因此无需论及在与交易相关联的服务中使用的其他技术。因此，本公开的实施例能够防止未知和/或恶意的、未授权方在数据安全系统内生成不需要的服务或生成垃圾邮件。

[0114] 根据本公开的实施例，作为一构思，可以通过移除密码并且通过用关于本公开的实施例而描述的模型替换密码来创建更安全的信息社会。本公开的实施例可能包含人类或

设备(例如,人工智能(AI)设备、机器人设备等)使用的所有信息系统,从而可以预先防止由用户自身引起的问题。本公开的实施例能够解决由过时技术引起的弱化保护和弱数据安全性问题,从而使未来信息社会对于其公民更加可靠和安全,使得自动信息系统更加独立和可靠地运行。因此,本公开的实施例易于用于例如银行设备和"金融科技"系统中,该系统需要极高程度的数据安全性以避免盗窃或欺诈;"金融科技"是金融银行技术的缩略词。本公开的实施例还易于用于有必要进行保护以免受第三方黑客攻击的关键基础设施,例如响应于随时改变的电力需求和/或随时改变的发电容量,在智能电网电力系统和网络中提供的负载响应。

[0115] 本公开的实施例使得与通信方相关联的用户能够以用户的名称(即,"用户名")的方式安全地登录由另一通信方提供的给定服务,在登录进程的任何阶段都不发送用户或密码的标识。通过采用这种方法,用户可以保持匿名。此外,通过采用这一方法,则无需使用加密连接,因为在登录(即,验证)过程中不得使用或发送可能对用户造成伤害或可能削弱提供给定服务的通信方的数据安全性的信息。可以理解的是,可以选择性地通过使用未加密的连接来执行登录,这正是由于要传递的信息并不重要,而信息本身也可以被加密,在这种情况下,只需要发送从密钥代码列表中使用的密钥的索引,以支持通信系统内部的安全数据交换。

[0116] 根据本公开的实施例,密码的使用被替换为数字密钥代码列表,数字密钥代码列表被设置为无需给定用户的任何动作而自动运行。

[0117] 本公开的实施例使得能够以考虑到国家的地方法规的方式实现登录 (即,验证)过程,前提是该国的当局有机会为其公民生成供官方使用的加密密钥对。与在当代信息社会中进行的各方之间的通信相比,这样的实施例实现了相当大的进步。此外,本公开的实施例使得也可以在离线操作模式下安全地登录。这种离线登录过程可以成功地完成,例如,在用户设备上,即使加密密钥对的生产者没有网络连接。

[0118] 本公开的实施例涉及困扰现代数据安全系统的安全漏洞的问题;因此,本公开的实施例能够通过采用仅能够使用一次的一次性密钥完全替代使用密码的需要。

[0119] 因此,通信方不一定需要建立和维护当前基于密码的实现中必需的信任关系。在本公开的实施例中,信任关系仅需要存在于每个通信方和密钥的生产者之间,即可信第三方。这样的可信第三方可以是一般公认的公证人或认证机构,取决于给定服务的生成地点和提供服务的人员。

[0120] 本公开的实施例使得可以经由使用公用互联网(因特网协议,IP) 安全地进行交互,而不必担心上述对安全性的威胁,这是因为敏感的登录(即,验证)信息,例如用户标识、电子邮箱地址或密码不是以加密形式或未加密形式、或是单向哈希形式中的任一形式进行传送。在本公开的实施例中,无需利用以下任何一种:交互中的超文本传输安全协议(HTTPS)、安全套接字层(SSL)或虚拟专用网络(VPN)保护。此外,在本公开的实施例中,时间事件ID(例如"认证令牌")不一定被传送;这样的时间事件ID易于被意图跟踪用户的用户设备的使用时间和地点的恶意方滥用。

[0121] 在希望当前登录会话在预定时间段内或直到满足预定目标为止保持开放的情况下,这种"认证令牌"可以以"会话令牌"的形式用于本公开的实施例中。如前所述,会话令牌是生成并从服务器发送到客户端以标识服务器和客户端之间的当前交互会话的唯一标识

符。使用这样的会话令牌是有利的，因为客户端只需要存储和处理会话令牌，而所有会话数据都链接到会话令牌并存储在与服务器相关联的数据库中。

[0122] 仅出于说明目的，现在将考虑根据本公开的实施例的没有密码的登录(即，验证)过程的示例实现，其中登录(即，验证)过程是在两个通信方之间执行，即客户端和服务器。在示例实现中，登录(即，验证) 过程分两个阶段执行，如下所示：

[0123] 阶段1：

[0124] 在阶段1中，数字密钥代码列表由客户端、服务器或可信第三方中任何一个产生。可选地，为数字密钥代码列表分配序列号，例如“abc-123”。

[0125] 通信方被提供相同或兼容的(即，能够协同使用以实现本公开的实施例)包括相同密钥和引用密钥的索引的数字密钥代码列表的副本。为此目的，使用安全的传输模式将数字密钥代码列表首次传递给通信方。例如，安全的传输模式可以通过基于公钥基础设施(PKI)的加密通信来实现，例如，诸如古鲁洛奇微系统公司的专有KWallet®，或通过已知的良好隐私(PGP®)。

[0126] 作为另一示例，数字密钥代码列表可以通过使用加密消息的文件传输来传递，例如，诸如近场通信(NFC)或蓝牙®，只要完全确定这样的文件传输可以安全地执行。

[0127] 作为又一示例，数字密钥代码列表可以经由未加密的存储卡，例如 USB存储设备(通俗地称为“USB记忆棒”)以挂号信的形式传递。

[0128] 在使用数字密钥代码列表之前，通信方必须确保数字密钥代码列表的生产者是可信和授权的一方，并且不受恶意方的阻碍。这一点在数字密钥代码列表是通过数据通信网络传送的情况下尤其重要，但是在数字密钥代码列表是物理上直接从另一个用户接收到的情况下也很重要。应当理解，绝对不应使用不可信的数字密钥代码列表。

[0129] 例如，当使用知名的PGP®时，给定用户和公共加密密钥的验证者之间存在信任关系，而当使用古鲁洛奇微系统公司的KWallet®时，发送方与数字密钥代码列表的生产者之间存在信任关系。

[0130] 这里要注意的是，每当需要用新的数字密钥代码列表替换现有的数字密钥代码列表时，或者在通信方还没有共同的数字密钥代码列表即同一个数字密钥代码列表的相同副本的情况下(在这种情况下，只要数字密钥代码列表的生产者是已知和可信的，就需要创建数字密钥代码列表)，都将重复阶段1。如果正在使用的现有数字密钥代码列表即将结束，即只剩下少量未使用的密钥，则当仍剩余未使用的密钥时，可选地传递新的数字密钥代码列表并达成一致；这种操作方式区别于已知类型的数据安全系统。在这种情况下，通过使用留在现有的数字密钥代码列表中的至少一个未使用的密钥，可以执行从一个通信方向另一个通信方或从可信第三方向两个通信方传递新的数字密钥代码列表而不会有安全问题。

[0131] 可选地，除了在使用之后被处置之外，如上所述，密钥的效力有时间限制，以提供额外程度的安全保护。可选地，整个密钥代码列表的效力是有时间限制的，需要定期更新密钥代码列表。

[0132] 至于技术实现，例如，登录(即，验证)仅允许在拥有同一个数字密钥代码列表的相同副本或至少相同密钥的通信方之间进行。因此，本公开的实施例使得可以偏离传统的基

于密码的登录(即,验证)过程,并且生成要在用户组和软件组件组之间使用的密钥。这增强了通信方之间的数据通信的安全性,因为只有确定的已知通信方可以尝试登录。

[0133] 阶段2:

[0134] 在阶段2中,无论使用哪种登录方法,通信方都能够登录到彼此的服务,例如如前所述。在示例中,使用了未加密连接中的超文本传输协议(HTTP)认证,以便与已知的现有技术相比更清楚地阐明根据本公开实施例的数据安全系统的使用场景以及如此实现的相应益处。

[0135] 在下文中,为方便起见,将未加密连接中的HTTP认证中的数据安全系统的使用场景指定为"HTTP KWallet®认证"。

[0136] 在示例中,客户端的用户设备(下文中用缩写形式"C"表示)与由服务器(下文中用缩写形式"S"表示)产生的服务进行通信。

[0137] 在示例中,用户设备"C"使用传统的HTTP协议经由TCP端口80 连接到服务器"S"提供的服务,因此不使用SSL加密。用户设备"C"向服务器"S"发送HTTP请求;默认情况下,HTTP请求设置为使用HTTP KWallet®认证方法。

[0138] 然后,用户设备"C"继续等待来自服务器"S"的响应,以便被通知请求是否成功。根据HTTP标准,默认成功响应代码(参见参考文献 [10])为"HTTP 200OK"。

[0139] 就此而言,服务器"S"处理从用户设备"C"接收的请求,并验证请求中使用的HTTP KWallet®认证方法。可选地,HTTP请求定义以下至少一个(例如,仅一个、至少两个、至少三个、至少四个等等):

[0140] (i)数字密钥代码列表用于登录(即,验证)过程;

[0141] (ii)用户设备"C"使用的数字密钥代码列表的序列号;

[0142] (iii)用户设备"C"用于加密登录(即,验证)信息的密钥的密钥索引;以及

[0143] (iv)经加密的附加信息。

[0144] 服务器"S"然后验证:

[0145] (a)所接收的序列号是否与服务器"S"所具有的数字密钥代码列表匹配,以及

[0146] (b)所接收的密钥索引是否与服务器"S"所具有的数字密钥代码列表中的密钥匹配。

[0147] 如果找到匹配的密钥,则服务器"S"验证登录过程的真实性和正确性,并通过使用密钥来解密经加密的附加信息。

[0148] 如果在验证过程中发生错误,则服务器"S"可选地根据默认HTTP 标准过程将HTTP响应状态码"HTTP 401未认证"发送到用户设备"C"。或者,可选地,可以发送一些其他响应,例如由HTTP KWallet®认证方法确定的响应,其中这样的响应定义了通信方与HTTP KWallet®认证方法协同运行的方式。

[0149] 例如,在由古鲁洛奇微系统公司开发的Starwindow®登录(即,验证) 过程中,加密信息可选地包括用户的唯一用户标识,其在Starwindow®过程中是用户的个人电子邮箱地址。"Starwindow®"是由古鲁洛奇微系统公司制造的专有软件产品。

[0150] 在操作中,验证加密信息以与所使用的数字密钥代码列表相关联。这足以检测可

能的破解尝试和未授权使用，由于Starwindow®是数字密钥代码列表的生产者，因此可以验证登录(即，验证)尝试中使用的序列号是否属于尝试登录的用户。这使得Starwindow®过程能够排除序列号所引用的数字密钥代码列表被并不拥有数字密钥代码列表的未授权用户使用。

[0151] 此外，可选地，对于本公开的实施例，可以使用任何可想到的消息或甚至指示日期和时间的字符序列作为附加信息(即，加密信息)。这些消息可选地用于替换实际的用户标识。或者，可选地，只要其他通信方或可信第三方能够识别消息，这些消息就与实际用户标识相结合。

[0152] 应当理解，为了使用HTTP KWallet®认证方法，仅发送项目(i)和 (iii)的信息就足够了，即如果两个通信方都已经接收到仅用于某个专门目的、通过HTTP KWallet®认证方法明确定义的数字密钥代码列表，则定义数字密钥代码列表用于登录(即，验证)过程以及定义使用密钥索引以提供用户设备“C”要使用的密钥。

[0153] 可选地，在本公开的实施例中，使用来自密钥代码列表的密钥，其可以用于若干需求，例如认证、登录和数据加密。

[0154] 例如，如果HTTP KWallet®认证方法仅使用一个数字密钥代码列表，则不需要发送数字密钥代码列表的序列号。作为另一示例，如果密钥已经被用于加密对于数据通信的运行必不可少的一些其他信息，诸如响应信息，则不需要发送加密的登录信息。

[0155] 此外，仅出于说明目的，现在将考虑登录(即，验证)过程的具体实现示例，其中用户设备“C”是在服务器“S”处自行注册的Starwindow®终端设备，使用上述HTTP KWallet®认证方法而非已知的标准HTTP基本和摘要访问认证方法(参见参考文献[11])。用户设备“C”向服务器“S”发送HTTP GET消息。HTTP KWallet®认证方法发信号作为授权信息的第一参数，例如数字密钥代码列表的64位序列号；应当理解，当实现本公开的实施例时，可以可选地使用其他长度的序列号。授权信息的第二参数是引用从数字密钥代码列表使用的密钥的索引，其在示例中引用数字密钥代码列表的第一时隙“1”处的密钥。授权信息的第三参数是加密的登录信息，登录信息是登录尝试发生时的日期和时间，可选地与Starwindow®用户标识字符串一起使用，而该字符串已使用第二参数引用的密钥进行加密。除加密外，第三参数也已转换为十六进制格式。在下面的示例中，登录信息使用96个字符。

[0156] 在验证授权信息之后，服务器“S”以标准HTTP结果代码“200OK”回复，表明注册已成功完成。

[0157] C:GET/signal/device/register/5776046 HTTP/1.1<cr><lf>

[0158] C:Host:signal.starwindow.net<cr><lf>

[0159] C:Authorization:KWallet 0123456789ABCDEF 1 06BE6D5A3E5D471EA3687088F647A54E214E284473C0773A00CA 46BE59982E236D3B75794555E8B2D292AA3E3787386C<cr><lf>

[0160] C:<cr><lf>

[0161] S:HTTP/1.1 200OK<cr><lf>

[0162] S:Date:Fri,08Jul 2016 06:29:14GMT<cr><lf>

[0163] S:Access-Control-Allow-Origin:*<cr><lf>

[0164] S:Content-Type:application/xml<cr><lf>

[0165] S:Content-Length:290<cr><lf>

[0166] S:Server:Starwindow Signal<cr><lf>

[0167] S:<cr><lf>

[0168] S:<290bytes of response content>

[0169] 另外,可选地,服务器“S”生成会话令牌,会话令牌标识服务器“S”与用户设备“C”之间的当前交互会话,并且将指示会话令牌的信息作为具有附加的“WWW-Authenticate”字段的HTTP响应头部的一部分进行发送(即,除了200之外,例如401),其描述所使用的数字密钥代码列表、加密密钥的密钥索引和经加密的会话令牌。例如,“WWW-Authenticate”字段可以表示如下:

[0170] WWW-Authenticate:realm=”restricted”,token=”0123456789ABCDEF2E367FA5E”

[0171] 然后,客户端“C”向服务器“S”发送后续数据以及会话令牌,其中至少会话令牌以加密形式发送。这使得服务器“S”能够在当前交互会话期间将后续数据识别为有效通信。

[0172] 第二方面,本公开的实施例提供了一种操作数据安全系统的方法,数据安全系统至少包括经由数据通信设置相互联接的第一方和第二方,其中数据通信设置可操作为提供用户认证和/或用户登录,上述方法包括:

[0173] (a)提供第一方和第二方至少一个数字密钥代码列表的相同或相互兼容的副本,数字密钥代码列表包括密钥和引用密钥的索引;

[0174] (b)设置第一方使其可操作为向第二方传递认证消息,认证消息包括要导出的密钥的索引、要导出密钥的数字密钥代码列表的唯一标识符 (ID)、以及指示下列中至少一个的附加信息:与第一方相关联的唯一用户ID、先前从第二方接收的会话令牌、尝试用户认证和/或用户登录的日期和时间,其中附加信息以加密形式提供;以及

[0175] (c)设置第一方和第二方使得可操作为:当在二者间执行数据通信以用于提供用户认证和/或用户登录时使用密钥,密钥是基于认证消息中的索引从数字密钥代码列表导出的;以及在使用后处置密钥,其中密钥设置为在第一方和第二方之间仅能够使用一次。

[0176] 可选地,使用其索引在认证期间传递的精确的加密密钥来加密附加信息。或者,可选地,使用一些其他加密密钥来加密附加信息,例如密钥代码列表中的下一个密钥,在这种情况下,接收方已经知晓使用下一个密钥这一事实。或者,可选地,附加信息使用另一加密密钥进行加密,其索引是单独传递的。

[0177] 应当理解,如前所述,方法易于实现为连续的过程,使得第一方和第二方之间的数据通信可选地使用来自数字密钥代码列表的一个或多个其他密钥加密。可选地,就此而言,密钥针对在第一方和第二方之间传送的每个消息而改变,并且它们的索引被传递或者被接收方隐含地知道,例如当密钥以特定顺序使用时。这可以防止在数据通信中发生中间人攻击。换而言之,即使恶意第三方设法劫持认证消息,恶意第三方也无法与接收方进行数据通信,因为恶意第三方无法访问定义了授权方之间的后续通信的数字密钥代码列表。

[0178] 根据本公开的实施例,上述方法包括:将密钥设置成被选择为供以下任何一个使

用:第一方、第二方或可信第三方。

[0179] 根据本公开的实施例,上述方法包括使第一方和第二方相互授权和认证。

[0180] 根据本公开的实施例,上述方法包括将数字密钥代码列表设置成由第一方或第二方提供。

[0181] 根据本公开的另一实施例,上述方法包括将数字密钥代码列表设置成由可信第三方提供。

[0182] 可选地,上述方法包括:当数字密钥代码列表由可信第三方提供时,设置第一方使得可操作为匿名地执行数据通信。

[0183] 根据本公开的实施例,上述方法包括:设置数据安全系统使得可操作为允许基于与第一方和第二方相关联的用户的生物识别来访问数字密钥代码列表。

[0184] 可选地,上述方法包括设置数据安全系统使得可操作为:在发现安全性已受到变得可供未授权第三方使用的数字密钥代码列表有关的信息的危害时,停用给定数字密钥代码列表。这种停用可选地响应于停用命令而实现,包括要被停用的给定数字密钥代码列表的标识。可选地,停用命令由以下至少一个发出:第一方、第二方、负责监督发生在第一方和第二方之间的通信的安全性的第三方。

[0185] 此外,可选地,上述方法包括设置数据安全系统使得可操作为:将到期时间与给定数字密钥代码列表相关联,以及在到达到期时间时,停用给定数字密钥代码列表。

[0186] 第三方面,本公开的实施例提供了一种计算机程序产品,包括其上存储有计算机可读指令的非暂时性计算机可读存储介质,计算机可读指令可由计算机化设备执行,计算机化设备包括用于执行根据前述第二方面的方法的处理硬件。

[0187] 可选地,计算机可读指令可从软件应用程序商店下载,例如,从“应用商店(App store)”下载到计算机化设备。

[0188] 接下来,将参考附图描述本公开的实施例。

[0189] 参考图1,提供了根据本公开实施例的数据安全系统100的示意图。数据安全系统100包括经由数据通信设置相互联接的第一方102和第二方104。向第一方102和第二方104提供数字密钥代码列表的相同副本,如图1中的106a和106b分别所示。可选地,还具有与第一方102和第二方104协同操作以提供数字密钥代码列表106c的第三方112。

[0190] 第一方102和第二方104可操作为:当在其间执行认证、登录和数据通信时,分别使用来自数字密钥代码列表106a和106b的密钥,并在使用后处置密钥。密钥设置为在第一方102和第二方104之间仅能够使用一次。可选地,密钥的效力是有时间限制的,以增加数据安全系统100 的安全性。

[0191] 在操作中,第一方102发送认证消息108,基于认证消息108,第二方104发送指示认证是否成功的响应110。除了认证,消息108也可以用于登录(到服务)。

[0192] 图1仅仅是一个示例,其不应不适当地限制本文权利要求的范围。应当理解,数据安全系统100的具体指定是作为示例提供的,而不应解释为将数据安全系统100限制为通信方的具体数量、类型或设置。还可以涉及一组通信方,其中所有通信方因而使用具有相同ID的密钥代码列表。本领域技术人员将认识到本公开的实施例的许多变化、替代和修改。

[0193] 继续参考图2A,提供了描述根据本公开的实施例的操作数据安全系统,例如数据安全系统100(包括经由数据通信设置相互联接的第一方和第二方)的方法的步骤的流程

图。方法被描述为逻辑流程图中的步骤集合，其代表可以以硬件、软件或其组合实现的一系列步骤，例如如前所述。

[0194] 在步骤202，即关于密钥代码列表的接收，向第一方和第二方提供数字密钥代码列表的相同或相互兼容的副本，数字密钥代码列表包括密钥和引用密钥的索引。

[0195] 在步骤204，即关于认证过程，设置第一方使其可操作为向第二方传递认证消息，认证消息包括要导出的密钥的索引、要导出密钥的数字密钥代码列表的唯一标识符(ID)、以及指示下列中至少一个的附加信息：与第一方相关联的唯一用户ID、先前从第二方接收的会话令牌、尝试用户认证和/或用户登录的日期和时间，其中附加信息以加密形式提供。

[0196] 此外，设置第一方和第二方使得可操作为：当在其间执行数据通信时，使用来自数字密钥代码列表的密钥，并在使用后处置密钥。根据步骤204，密钥设置为在第一方和第二方之间仅能够使用一次。可选地，密钥的效力是有时间限制的，以增加数据安全系统100的安全性。

[0197] 步骤202至204仅仅是说明性的，并且在不脱离本文权利要求的范围而添加一个或多个步骤的情况下，还可以提供其他替代方案。

[0198] 继续参考图2B，提供了描述认证过程204的步骤的流程图。在步骤 206，第一方将认证消息发送给第二方，以进行登录，例如登录到第二方提供的服务。在已接收到合格响应之后，在步骤208，过程继续进行至登录过程，其中基于认证消息中的索引，从密钥代码列表中导出密钥。最后，在步骤210，处置使用过的密钥。

[0199] 可选地，第一方选择要使用的密钥，然后继续等待来自第二方的响应。然后，在使用之后或在响应到达之后，立即处置使用过的密钥。

[0200] 应当理解，方法易于实现为连续的过程，使得第一方和第二方之间的数据通信可选地使用来自数字密钥代码列表的一个或多个其他密钥来进行加密，如前所述。可选地，就此而言，密钥针对在第一方和第二方之间传送的每个消息而改变，并且它们的索引或被传递或被接收方隐含地知道，例如当密钥以特定顺序使用时。这可以防止在数据通信中发生中间人攻击。换而言之，即使恶意第三方设法劫持认证消息，恶意第三方也无法与接收方进行数据通信，因为恶意第三方无法访问定义了授权方(即第一方和第二方)之间的后续传送的数字密钥代码列表。

[0201] 步骤206至210仅仅是说明性的，并且在不脱离本文权利要求的范围而添加一个或多个步骤的情况下，还可以提供其他替代方案。

[0202] 继续参考图3，示出了根据本公开实施例的示例性认证消息的内容。

[0203] 如图3所示，认证消息包括数字密钥代码列表的唯一ID 302。认证消息还强制性地包括引用密钥的密钥索引304。

[0204] 另外，认证消息包括加密信息306。加密信息306包括以下至少一个：唯一用户标识信息308、指示发送认证消息的日期和时间的字符序列310、一个或多个其他消息312，例如，其他消息312包括先前从被传递认证消息的给定方接收的会话令牌。此外，可选地，认证消息包括指示所使用的认证方法的信息，其中信息由314表示。

[0205] 此外，应当理解，认证消息的内容可在认证消息内以任意顺序提供。图3仅仅是一个示例，不应该不适当地限制本文权利要求的范围。本领域技术人员将认识到本公开实施例的许多变化、替代和修改。

[0206] 在不脱离由所附权利要求限定的本公开的范围的情况下,可以对前述的本公开的实施例进行修改。用于描述和要求保护本公开的诸如“包括”、“包含”、“结合”、“由.....组成”、“具有”、“是”等的表达旨在以非排他的方式解释,即允许未明确地描述的项目、组件或元素的存在。对单数的引用也应解释为涉及复数;例如,“至少一个”在一个例子中表示“一个”,在另一个示例中表示“多个”;此外,“两个”和类似的“一个或多个”应以同样的方式解释。所附权利要求中的括号内包括的数字旨在帮助理解权利要求,并且不应以任何方式解释为限制这些权利要求所要求保护的主题。

[0207] 短语“在一个实施例中”、“根据实施例”等通常意味着短语后的具体特征、结构或特性包括在本公开的至少一个实施例中,并且可以包括在本公开的多于一个的实施例中。重要的是,这些短语不一定指的是同一个实施例。

[0208] 参考文献

[0209] [1]基本访问认证-维基百科(访问于2016年7月14日);URL: https://en.wikipedia.org/wiki/Basic_access_authentication

[0210] [2]摘要访问认证-维基百科(访问于2016年7月14日);URL:https://en.wikipedia.org/wiki/Digest_access_authentication

[0211] [3]Kerberos协议-维基百科(访问于2016年7月14日);URL: https://en.wikipedia.org/wiki/Kerberos_(protocol)

[0212] [4]NT局域网管理器-维基百科(访问于2016年7月14日); URL:https://en.wikipedia.org/wiki/NT_LAN_Manager

[0213] [5]开放授权-维基百科(访问于2016年7月14日);URL: https://en.wikipedia.org/wiki/OAuth

[0214] [6]开放ID-维基百科(访问于2016年7月14日);URL: https://en.wikipedia.org/wiki/OpenID

[0215] [7]SPNEGO-维基百科(访问于2016年7月14日);URL: https://en.wikipedia.org/wiki/SPNEGO

[0216] [8]安全远程密码协议-维基百科(访问于2016年7月14日); URL:https://en.wikipedia.org/wiki/Secure_Remote_Password_protocol

[0217] [9]传输层安全协议-维基百科(访问于2016年7月14日);URL: https://en.wikipedia.org/wiki/Transport_Layer_Security#Client-authenticated _TLS_handshake

[0218] [10]HTTP状态码列表-维基百科(访问于2016年7月14日);URL:https://en.wikipedia.org/wiki/List_of_HTTP_status_codes

[0219] [11]RFC 2617-HTTP认证:基本及摘要访问认证(访问于2016 年7月14日);URL: https://tools.ietf.org/html/rfc2617

[0220] [12]GNU隐私保护-维基百科(访问于2016年8月29日);URL: https://en.wikipedia.org/wiki/GNU_Privacy_Guard

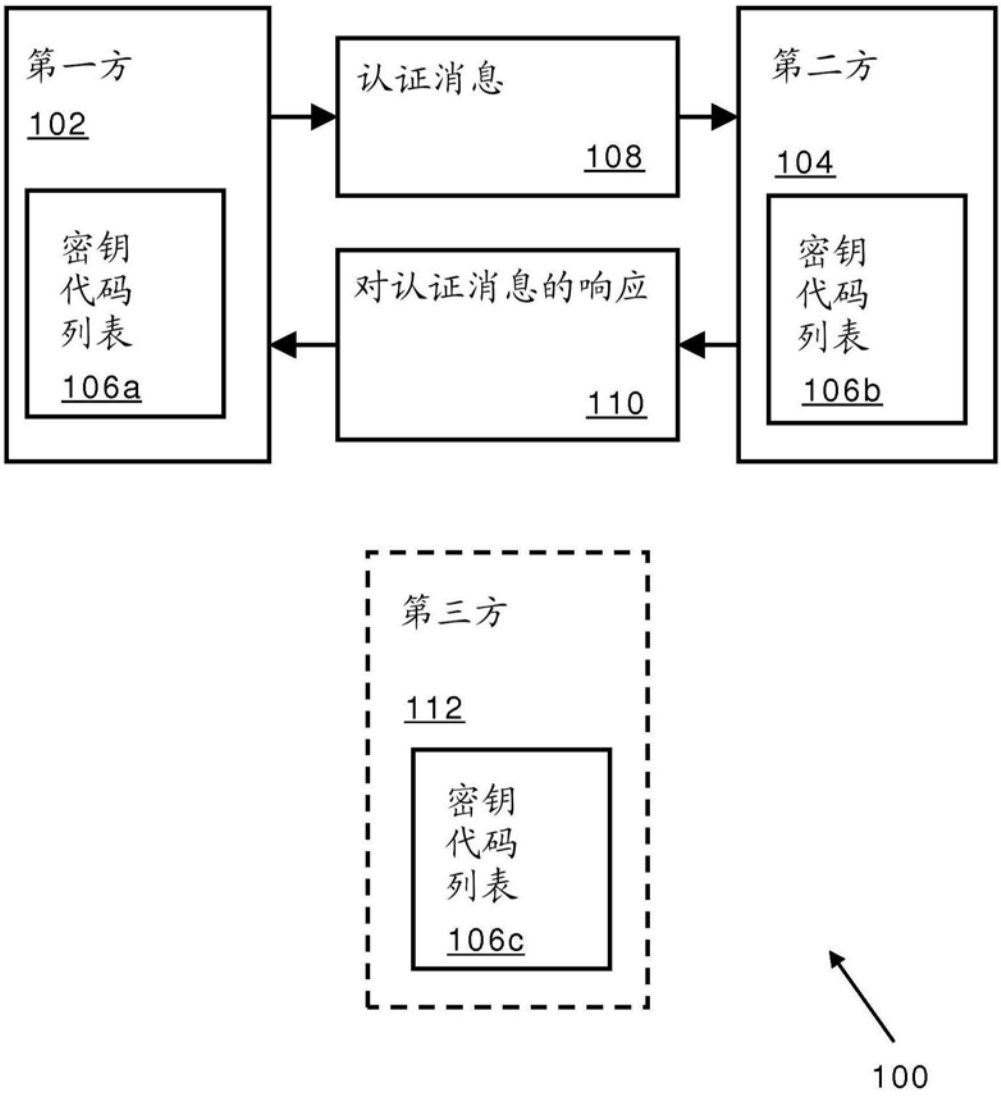

第一方
102
密钥
代码
列表
106a
认证消息
108
对认证消息的响应
110
第二方
104
密钥
代码
列表
106b
第三方
112
密钥
代码
列表
106c
100

图1

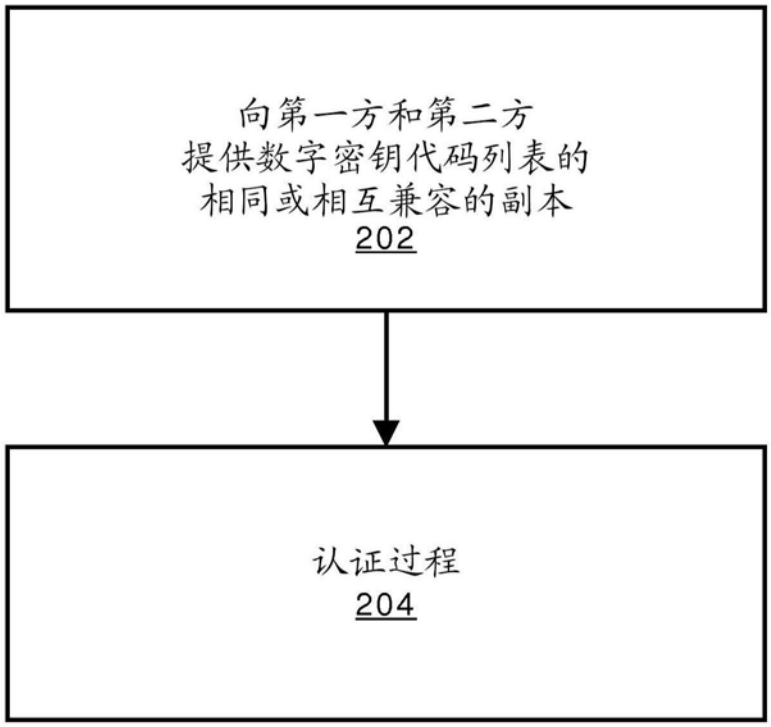



图2A

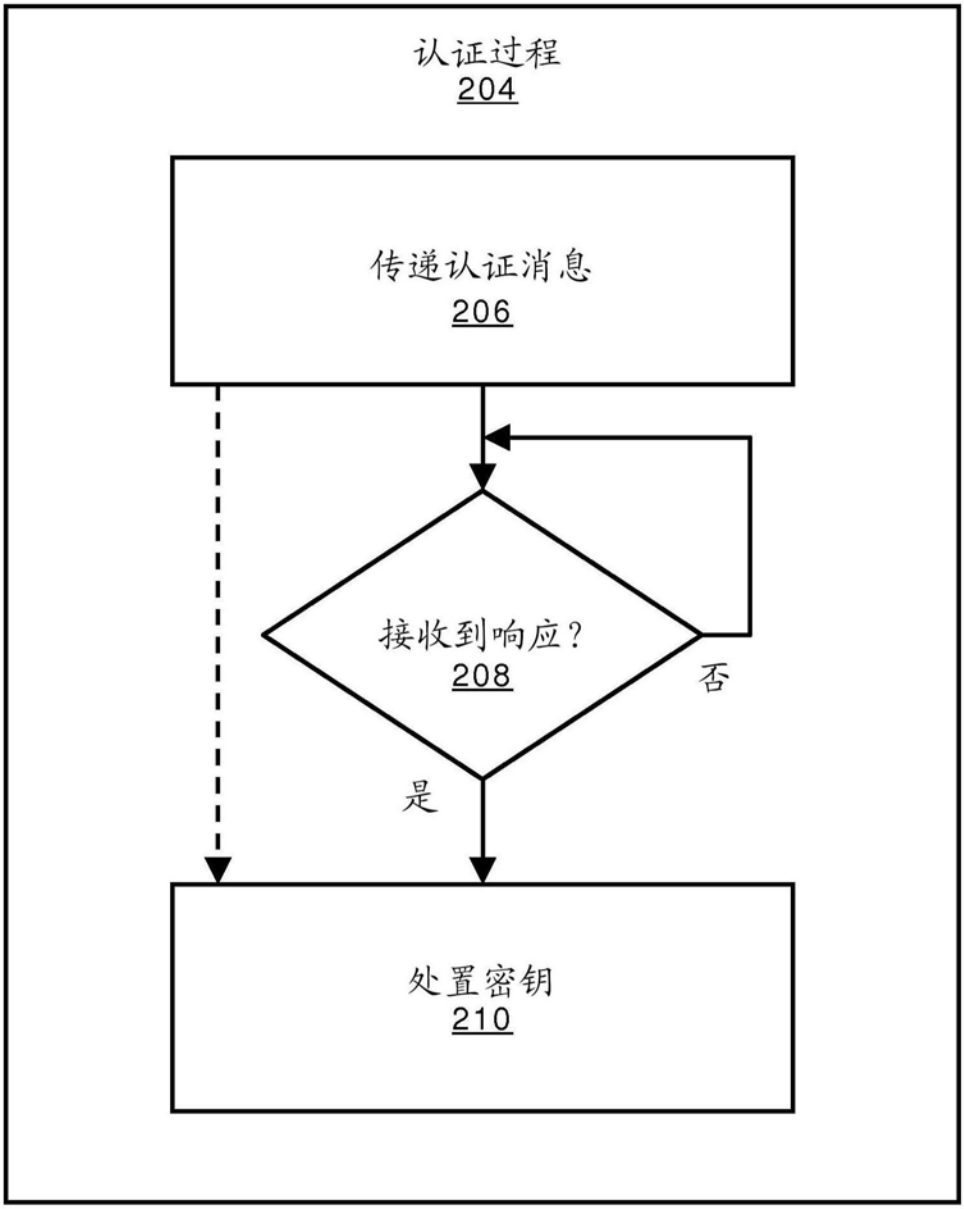



图2B

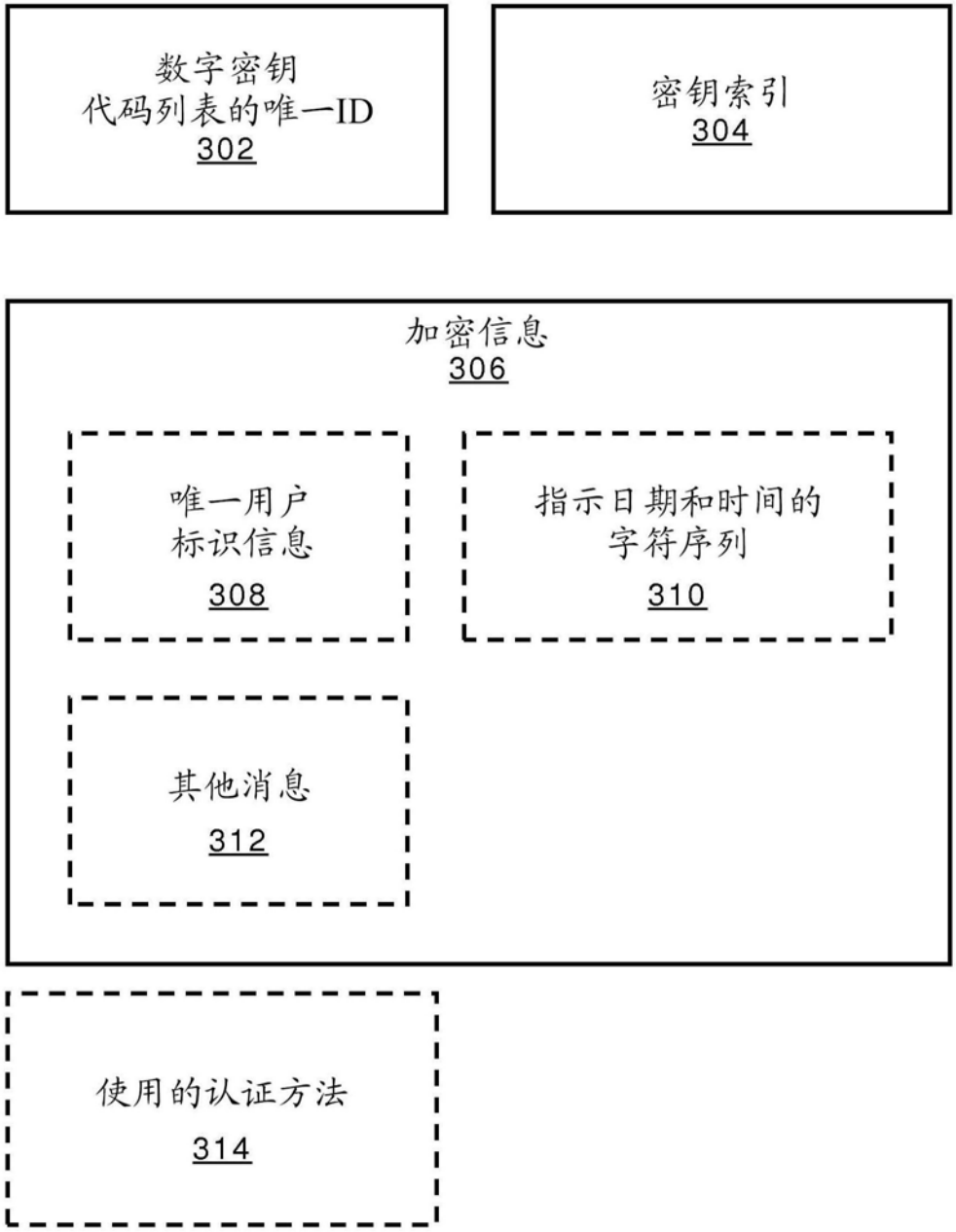

数字密钥
代码列表的唯一ID
302
密钥索引
304
加密信息
306
唯一用户
标识信息
308
指示日期和时间的
字符序列
310
其他消息
312
使用的认证方法
314

图3